404 Solution <= 2.35.17 - Missing Authentication to Sensitive Information Exposure

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2024-11094
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-11-16 10:15:04 UTC
Updated	2026-04-08 19:19:34 UTC
Description	The 404 Solution plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2

Risk And Classification

Primary CVSS: v3.1 5.3 MEDIUM from security@wordfence.com

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

EPSS: 0.003960000 probability, percentile 0.604530000 (date 2026-04-13)

Problem Types: CWE-488 | CWE-488 CWE-488 Exposure of Data Element to Wrong Session

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
3.1	CNA	DECLARED	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

ntegrity

None

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Aaron13100	404 Solution	affected 2.35.17 semver	Not specified
ADP	Aaron13100	404 Solution	affected 2.35.17 custom	Not specified

References

Reference	Source	Link
plugins.trac.wordpress.org/changeset	security@wordfence.com	plugins.trac.wordpress.org
www.wordfence.com/threat-intel/vulnerabilities/id/d738be73-2573-4fb8-b6f0-768a0...	security@wordfence.com	www.wordfence.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Max Boll (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-11-15T20:57:53.000Z	Disclosed

There are currently no legacy QID mappings associated with this CVE.